PCAP Converter Instructions

Team Gamma – Antony Gillette

April 16, 2017

Dependencies

1) GCC (or equivalent C compiler)
2) Make
3) pcap development libraries (apt-get install libpcap-dev or the equivalent)
4) pcap_to_ipv4_udp.c and the included Makefile
5) Hex reader such as xxd to see output

Note: Tested on Ubuntu 14.04, grey highlights represent commands in terminal

Instructions

To build and run **pcap_to_ipv4_udp.c** (extracts IPv4 UDP packets from pcap files):

1) make ip
    a. To build without make: gcc pcap_to_ipv4_udp.c -lpcap -o ptiu
2) ./pitu <*input_file*> <*output_file*>
    a. *input_file* represents the path to a pcap file
    b. *output_file* represents the filename of the IPv4/UDP packet output
    c. Example: ./pitu sample_capture.pcap ipv4_udp.bin

To scroll through file output:

1) xxd ipv4_udp.bin | less

Notes

1) To build on Windows, WinPcap is needed and can be downloaded here: https://www.winpcap.org/devel.htm
   To set up WinPcap for compiling with C programs, see the following: https://www.winpcap.org/docs/docs_40_2/html/group__wpcapsamps.html

2) A wide selection of example pcap files for testing can be downloaded here: http://www.netresec.com/?page=PcapFiles
3) This PCAP converter expects non-corrupted PCAP files, and filters out all but IPv4 packets with UDP payloads by analyzing the protocol byte in the IPv4 headers and deleting packets without the UDP protocol byte